Enterprise Risk Management

Emanuels, Jim; de Munnik, Wilmar

Published in:
Maandblad voor Accountancy en Bedrijfseconomie

Enterprise Risk Management

een risicobeheersingssyteem voor organisaties

Jim Emanuels en Wilmar de Munnik

SAMENVATTING Het doel van het risicobeheersingssysteem is om met de gewenste mate van zekerheid te kunnen stellen dat de organisatiedoelstellingen worden bereikt. Het risicobeheersingssysteem richt zich op een viertal categorieën van doelstellingen te weten "strategisch", "operationeel", "wet- en regelgeving" en "betrouwbaarheid van informatie". Het feit dat een organisatie beschikt over een risicobeheersingssysteem betekent niet dat de organisatiedoelstellingen daadwerkelijk worden gerealiseerd, maar dat transparant wordt gemaakt welke risico's met de doelstellingen samenhangen en welke beheersingsmaatregelen getroffen worden. Er zijn meerdere methoden om risico's te inventariseren waarbij een combinatie van de methoden (kwalitatief en kwantitatief) toegepast kan worden om een zo hoog mogelijke effectiviteit en efficiency te bereiken. Daarnaast is het van groot belang om als onderdeel van het risicobeheersingssysteem aandacht te besteden aan de verankering van het risicomanagementproces in een organisatie (cultuur, structuur, competenties en techniek).

1 Inleiding

Door het tekortschieten van de interne beheersing met betrekking tot de financiële informatievoorziening is een reeks grote boekhoudschandalen opgetreden bij beursgenoteerde ondernemingen zoals Ahold, Worldcom, Tyco, Enron, Parmalat, etc. (Emanuels, 2005).
Deze recente ontwikkelingen hebben ertoe geleid dat overheden en toezichthouders wereldwijd maatregelen hebben getroffen om het toezicht op het management te verbeteren. Hiermee wordt beoogd op korte termijn de kans op nieuwe schandalen zo klein mogelijk te maken. Dit wordt gezien als essentiële voorwaarde voor de belanghebbenden om vertrouwen in bestuur en toezicht te kunnen stellen. In Nederland heeft de wetgever ervoor gekozen om voor beursgenoteerde ondernemingen toepassing van de Code Tabaksblat af te dwingen.

Prof. Dr. J.A. Emanuels RA is partner van Tacstone La Rive. W.G. de Munnik RA is controller bij de Corporatieholding Friesland. Beide zijn tevens verbonden aan de Vakgroep Accountancy van de Rijksuniversiteit Groningen, als hoogleraar respectievelijk universitair docent Bestuurlijke Informatieverzorging.

De code bevat onder meer de bepaling dat: "… *het bestuur in het jaarverslag verklaart dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn*" (Commissie Corporate Governance, 2003, artikel II.1.4). Deze (gemotiveerde) verklaring van het bestuur is de zogenaamde "in control" statement.

De definitie in de Code Tabaksblat bevat ons inziens een theoretisch gezien overbodige toevoeging. Interne controle is immers een integraal onderdeel van het risicobeheersingssysteem, namelijk dat onderdeel dat gaat over het treffen van beheersingsmaatregelen die de betrouwbaarheid van (financiële) informatie waarborgen. In het vervolg van dit artikel zullen wij dan ook spreken over het interne risicobeheersingssysteem Volgens de code ligt het in de rede dat het bestuur in de verklaring aangeeft welk raamwerk of normenkader men heeft gehanteerd. Als voorbeeld wordt het COSO raamwerk voor interne beheersing genoemd. Dit dateert uit 1992, maar in het najaar van 2004 (dus na het definitief worden de Code Tabaksblat) kwam COSO met een nieuw framework, getiteld: "Enterprise Risk Management: Integrated Framework." (COSO, 1992 en 2004). Dit framework is ten opzichte van dat uit 1992 meer gericht op het organisatiebreed beheersen van risico's. De voorzitter van COSO, John Flaherty, kenschetst de ontwikkeling van COSO naar COSO ERM: "*As events have transpired in recent years, we've come to realize that we can't consider risk in a silo anymore.*" (Chapman, 2003).

In dit artikel gaan wij in op hoe Enterprise Risk Management (hierna ERM genoemd) als intern risicobeheersingssysteem toegepast kan worden, bijvoorbeeld bij de implementatie van de Code Tabaksblat. Hiertoe geven we in dit artikel een overzicht van het

systeem en de beoogde doelstellingen (2), behandelen vervolgens de opzet van het ERM proces (3) en de randvoorwaarden van het systeem (4). Ten slotte sluiten we in paragraaf 5 af met de belangrijkste conclusies.

2 De doelen van het ERM systeem

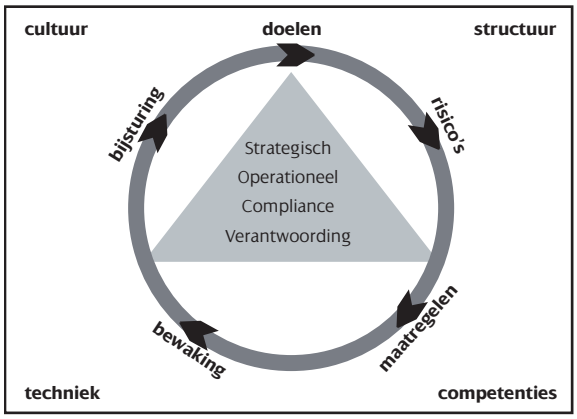
Het uitgangspunt voor dit artikel is dat het management van een organisatie verantwoordelijk is voor het behalen van de organisatiedoelstellingen en dat het met een hoge mate van waarschijnlijkheid (tegen reële kosten) deze doelstellingen wil behalen. Dit betekent overigens niet dat het management altijd zal streven naar het behalen van de organisatiedoelen, maar de beïnvloeding van het management tot het voeren van het gewenste beleid en de controle hierop zijn een agency-, respectievelijk een corporate governance vraagstuk, waarvan behandeling in dit kader te ver zou voeren.

Door toepassing van ERM wordt beoogd de risico's van het niet behalen van de doelstellingen te beheersen. Een ERM systeem zou op grond daarvan dus duidelijke toegevoegde waarde moeten hebben voor iedere organisatie. Een ERM systeem kan als volgt worden gedefinieerd:

"Het systeem dat het management in staat stelt om de relevante risico's, die het behalen van de doelstellingen van de organisatie bedreigen, te kunnen identificeren, te prioriteren, te analyseren en te beheersen" (Emanuels, 2005).

Onder een systeem verstaan we een doelmatig geordend geheel van bij elkaar horende entiteiten en hun onderlinge relaties. In figuur 1 is een schematische opbouw weergegeven van het ERM systeem op basis van de voorgaande definitie. Uit deze figuur blijkt dat het gaat om een proces met een aantal volgordelijke stappen dat functioneert binnen een kader van randvoorwaarden. De stappen in het proces zijn: bepalen van doelstellingen, inschatten van risico's, treffen van beheersingsmaatregelen, bewaken van de effectiviteit en het bijsturen indien nodig. Dit proces en de randvoorwaarden tezamen noemen wij het ERM systeem. In de praktijk betekent het dat een organisatie die ERM heeft doorgevoerd het in figuur 1 geschetste proces continu en beheerst doorloopt. De wijze waarop het proces ingevuld wordt en de wijze waarop de organisatie bijgestuurd wordt, is vooral een management control vraagstuk: veel delegatie of veel centrale uitvoering?, "strakke" beheersing (bijvoorbeeld door regelmatige en uitgebreide operational control) of "losse" beheersing (bijvoorbeeld door periodieke zelfevaluaties)? Het management control proces is het proces waarbij managers op alle niveaus binnen een organisatie ervoor zorgen dat de mensen aan wie zij leiding geven de door hen uitgezette strategie implementeren (Anthony en Govindarajan, 2002). In die zin is de effectiviteit van het management control systeem dus van invloed op de werking van het ERM systeem.

Figuur 1: Het ERM systeem



Het ERM systeem richt zich, zoals in figuur 1 aangegeven, op doelstellingen in de volgende categorieën:

- Strategie: op het allerhoogste niveau en gebaseerd op de missie;
- Operationeel: effectieve en efficiënte inzet van middelen;
- Rapportage: betrouwbaarheid van de informatievoorziening[1];
- Compliance: handelend in overeenstemming met wet- en regelgeving[2].

De indeling in risicogebieden draagt bij aan het (overzichtelijk) in kaart brengen van risico's en aan het gericht verzamelen van informatie die nodig is om de risico's te kunnen inschatten en te kunnen beheersen (Roth en Espersen, 2002). De te onderkennen risicogebieden kunnen verschillen per soort organisatie. Het risicogebied wet- en regelgeving (compliance) zal bijvoorbeeld bij financiële instellingen een belangrijkere rol spelen dan bij andere organisaties. Wezenlijk voor ERM is wel dat alle risico's die het realiseren van de doelstellingen van de organisatie beïnvloeden, object van beheersing zijn. ERM heeft daarmee qua benadering en startpunt een strategisch en integraal karakter.

3 Het ERM proces

In het voorgaande is beschreven welke categorieën van doelstellingen binnen ERM moeten worden

beheerst. Het volledig afdekken van deze gebieden is één belangrijk facet van integraal risicomanagement die de term *Enterprise* Risk Management rechtvaardigt. Een ander aspect is de inrichting van ERM als een *proces* dat van begin tot eind beheerst wordt. Dit proces kent voor alle vier genoemde gebieden dezelfde stappen die doorlopen worden. Deze stappen worden hierna toegelicht.

3.1 Het definiëren van de te beheersen doelstellingen

Doelstellingen worden op het hoogste (strategische) niveau geconcretiseerd vanuit de missie van de organisatie en de visie die de organisatieleiding heeft op het bereiken van die missie. Vervolgens wordt een strategie bepaald om deze doelstellingen te halen, die weer verder vertaald wordt in doelstellingen op operationele, rapportage- en compliancegebieden. Het ERM systeem is niet bedoeld om uitspraken te doen over de inhoudelijke wenselijkheid, aanvaardbaarheid of haalbaarheid van de doelstellingen. Het is in die zin waardevrij. De processen die de doelstellingen genereren zijn wel onderdeel van het systeem, omdat ze van voldoende kwaliteit moeten zijn om te waarborgen dat er relevante doelen worden nagestreefd met voldoende samenhang tussen en binnen alle categorieën. Onder relevantie verstaan we de feitelijke bijdrage aan de hoogste doelstellingen van de organisatie. Voorbeelden van management control processen die in dat kader beheerst moeten worden, zijn onder andere het strategievormingsproces, het business planningsproces en het budgetteringsproces (Anthony en Govindarajan, 2002). Instrumenten om deze processen te beheersen zijn talrijk. Bekend en algemeen toegepast is bijvoorbeeld de Balanced Business Scorecard. Met behulp van deze methodiek kunnen vanuit een misse/visie en strategie, doelstellingen worden geformuleerd voor operationele processen.

De gewenste waarde van de te beheersen doelstellingen is afhankelijk van de mate waarin een organisatie risico wil lopen (de mate van risicoafkeer). Ambitieuze doelstellingen gaan in het algemeen met meer onzekerheid over de haalbaarheid gepaard dan bescheiden doelstellingen.

Dit komt omdat bij ambitieuze doelstellingen "alles" goed moet gaan, zoals bij een schaatser die een wereldrecord probeert te rijden. De tolerantie voor verstoringen van buiten af en fouten in processen is veel kleiner. Bij minder ambitieuze doelstellingen kunnen tegenvallers opgevangen worden en kunnen fouten gecompenseerd worden. De mate waarin de organisatie geneigd is lagere doelstellingen te accepteren in ruil voor meer zekerheid, wordt risicoafkeer genoemd. Over het algemeen wordt voor een doelstelling door het stellen van een boven-/ondergrens een gebied afgebakend waarbinnen doelrealisaties (uitkomsten) nog als acceptabel worden beschouwd in relatie tot het aanvaarde risico. In specifieke gevallen kan ook sprake zijn van een boven- *en* een ondergrens.

Doelstellingen: een voorbeeld

De missie/visie van een onderneming is om marktleider te zijn binnen de bedrijfstak. De strategische doelstelling die hieraan gekoppeld is, is het realiseren van een marktaandeel van minimaal 50% binnen een periode van maximaal 2 jaar. De te volgen strategie is het introduceren van nieuwe producten binnen een bestaande markt. Vanuit deze strategie kunnen operationele doelstellingen worden geformuleerd zoals het ontwikkelen van minimaal 2 en maximaal 4 nieuwe producten, voor maximaal € 2 miljoen met een minimaal rendement op het geïnvesteerde vermogen van 10%.

3.2 Het bepalen van risico's

De definitie van een risico is de kans op het optreden van een gebeurtenis of omstandigheid die er toe kan leiden dat een doelstelling niet gehaald wordt (Committee of Sponsoring Organizations of the Treadway Commission, 2004). Een in deze zin relevante gebeurtenis of omstandigheid wordt in ERM termen aangeduid met een "event". Eerste stap bij het bepalen van risico's is dan ook het identificeren van mogelijke events die de haalbaarheid van de doelstelling negatief beïnvloeden. Er kan hierbij in de eerste plaats onderscheid gemaakt worden tussen interne en externe gebeurtenissen en omstandigheden. Interne gebeurtenissen en omstandigheden zijn de verantwoordelijkheid van de organisatie zelf, externe gebeurtenissen en omstandigheden ontstaan buiten de organisatie en maken deel uit van de context waarbinnen de organisatie moet opereren. Dit onderscheid is belangrijk, omdat het indicatief is voor de mate waarin het optreden van het event beïnvloed kan worden door maatregelen die ingrijpen in de eigen processen (interne beheersingsmaatregelen) en de mate waarin slechts op de gevolgen van de events kan worden geanticipeerd of gereageerd.

Vervolgens moeten wij de begrippen "impact" en "likelihood" introduceren. Onder impact wordt de invloed van een gebeurtenis of omstandigheid op de te bereiken doelstelling verstaan. Een gebeurtenis of omstandigheid met een geringe impact hoeft niet direct een risico in te houden, wanneer het de doelstelling nauwelijks negatief beïnvloedt. Likelihood staat voor waarschijnlijkheid en betreft de kans dat de rele-

vante gebeurtenis of omstandigheid feitelijk optreedt. Het resultaat van het bepalen van impact en likelihood is een onderbouwde kansverdeling per event, gerelateerd aan de gestelde doelen en per categorie (interne en externe gebeurtenissen en omstandigheden).

3.3 Het nemen van risicomitigerende maatregelen (risk response)

Op basis van de kansverdeling maakt de leiding van een organisatie keuzes in de aard en omvang van de te treffen maatregelen om de risico's terug te dringen. Daar waar de kans op een negatieve afwijking van de gestelde doelstelling groter is dan het risico dat de leiding wenst te lopen ("risk appetite"), moeten er maatregelen getroffen worden.

Essentieel is het onderscheid tussen maatregelen in generieke zin en beheersingsmaatregelen. Zo kan het afstoten van een slecht geleide deelneming een "risk response" zijn, maar dat geldt ook voor het aanstellen van een controller bij die deelneming. Alleen het laatste kwalificeert als het invoeren van een beheersingsmaatregel. Het afstoten van de deelneming is een besluit dat leidt tot een wijziging van het risicoprofiel van de organisatie, of met andere woorden tot een gewijzigd "inherent" risico (zie ook paragraaf 4).

De kosten van alle maatregelen, inclusief het ontwerpen, implementeren en uitvoeren van beheersingsmaatregelen kan gezien worden als "verzekeringspremie", net zo goed als onwenselijke risico's door extern verzekeren kunnen worden afgedekt. Het besluit om al dan niet tot het afdekken van risico's over te gaan, gaat dan ook altijd gepaard met een kosten-baten afweging die weer terugslaat op het gewenste risicoprofiel (risicoafkeer) van de organisatie.

3.4 Bewaking en Bijsturing

Deze stappen, die samen het logische eindpunt van het proces markeren, betreffen het periodiek testen van de beheersingsmaatregelen, het meten (traceren) van events die zich feitelijk voordoen en het analyseren naar oorzaak en impact. Het iteratieve karakter van het proces komt tot uitdrukking in de aansluiting tussen deze laatste stap en de eerdere stappen. Nadat is vastgesteld welke events zich hebben voorgedaan en wat de impact was, kan de risk response worden bijgesteld, maar ook kan de inschatting van impact en likelihood worden bijgesteld en zelfs kunnen doelstellingen herzien worden, als blijkt dat bepaalde risico's te groot of te moeilijk beheersbaar zijn.

Het ERM proces omvat het continu (sequentieel en iteratief) doorlopen van de beschreven stappen. Dit proces kan op verschillende niveaus binnen een organisatie worden toegepast. Als dit proces consequent en binnen een gehele organisatie is geborgd, is er sprake van een adequaat intern risicobeheersingsysteem.

In het voorgaande is uiteengezet dat het proces van ERM in een aantal stappen dient te worden doorlopen. Voor een uitgebreidere bespreking van de methoden en technieken die hierbij kunnen worden toegepast wordt verwezen naar Emanuels en De Munnik (2005).

4 Inbedding: de randvoorwaarden van het systeem

Zoals reeds aangegeven, is het noodzakelijk dat het ERM proces op zichzelf beheerst wordt. Hier is dus sprake van een meta-beheersingsdoelstelling: het ERM proces dient ertoe om doelstellingen op verschillende gebieden te beheersen, maar het proces zelf wordt ook beheerst. Het onderkennen van deze gelaagdheid in beheersingsdoelstellingen is belangrijk omdat het bepalend is voor de visie van het management en de buitenwereld op de vraag of een organisatie al dan niet "in control" is.

Bij de definitie van in control moet primair aansluiting gezocht worden bij de metabeheersingsdoelstelling. Concreet betekent dit dat een organisatie die verschillende risico's loopt en (nog) niet al die risico's adequaat heeft afgedekt, wel een in control statement kan afgegeven, er vanuit gaande dat zij zelf de risicoanalyse heeft uitgevoerd en ook maatregelen in gang heeft gezet om de geconstateerde onwenselijke "exposure" op te heffen. Immers, er is in dat geval sprake van gestructureerde uitvoering van het iteratieve risicomanagementproces. Een lezer van het in control statement van een dergelijke organisatie kan zelf vervolgens, naar zijn eigen maatstaven en voor zijn eigen doelen, beoordelen of het actuele risicoprofiel van de organisatie voor hem aanvaardbaar is. Een organisatie die daarentegen meent geen enkel materieel risico te lopen, maar deze conclusie uitsluitend baseert op een eenmalige inventarisatie van incidenten en een goedkeurende accountantsverklaring, is niet in control. Deze organisatie kan namelijk niet aantonen dat doelstellingen procesmatig continu beheerst worden. Met andere woorden: het door deze organisatie geschetste risicoprofiel is niet betrouwbaar en derhalve is een in control statement in dat geval voor een gebruiker ook ongeschikt om een oordeel op te baseren . Wordt het door de keuze voor deze definitie makkelijker om in control te zijn? Dat valt te betwijfelen. Zoals Paape (2003) ons inziens terecht stelt, is juist het inrichten van een permanent proces de grote uitdaging. Paape noemt dit de overgang van een statische naar een dyna-

mische risicomanagementexcercitie (Paape, 2003)
Het geheel van risicomanagementproces, tezamen met het meta-beheersingsproces en alle functies, taken en middelen die daarbij een rol spelen vormen het ERM systeem (zie ook figuur 1). Concreet onderscheiden we als randvoorwaarden binnen het systeem:

Risicobewustzijn (cultuur)
Er is organisatiecultuur nodig waarin wordt gedacht vanuit kansen en risico's en waarin men wordt uitgedaagd om risico's te beheersen wanneer ze nog beheersbaar zijn in plaats van wanneer het te laat is.

Opzet van het systeem en de organisatie van processen (structuur)
Het ERM systeem wordt verankerd op het hoogste niveau binnen de organisatie en de juiste opzet en werking ervan behoren tot de directe verantwoordelijkheid van de Directie of de Raad van Bestuur. In veel gevallen zien we nog wel dat binnen de directie de CFO de "risicomanagement" portefeuille heeft, maar gegeven het integrale karakter van ERM mag het duidelijk zijn dat er minstens een even grote betrokkenheid moet zijn van de executives die verantwoordelijk zijn voor de strategische, commerciële en operationele processen. Het zou daarom niet onlogisch zijn om de CEO of de voorzitter van de Raad van Bestuur met deze portefeuille te belasten.

De ERM processen moeten worden vertaald in taken die deels onderbracht worden in lijnfuncties (bijvoorbeeld als onderdeel van strategievorming) en deels in ondersteunde functies (bijvoorbeeld waar het gaat om testen van beheersingsmaatregelen en rapportage van de werking van de maatregelen). Een voorbeeld van een nieuw orgaan dat kan ontstaan bij het vormgeven van deze nieuwe structuur, is de risk identification-groep, waarin alle betrokken functies bijeenkomen om voortgang en acties te monitoren en ontwikkelingen te bespreken (Willemse et al., 2003).
In de keuze van een specifieke structuur spelen vraagstukken een rol als gewenste functiescheiding en specialisatie die kunnen leiden tot verschillende oplossingen voor verschillende organisaties, waarbij gehele of gedeeltelijke integratie met de bestaande planning- en controlcyclus voor de hand ligt.

Kennis en Vaardigheden (Competenties)
Risicodenken en risico-evaluatie vragen om specifieke kennis en vaardigheden. Het volstaat helaas niet om een risk manager aan te trekken die deze competenties bezit en ervaren is met ERM, omdat het proces in verschillende stadia vraagt om input, betrokkenheid en beslissingen van diverse functionarissen in de gekozen structuur, met name ook van lijnfunctionarissen. Deze zullen dus aanvullend opgeleid, getraind en beoordeeld moeten worden op deze aspecten van het managen van hun "business".

Hulpmiddelen (Techniek)
Afhankelijk van de complexiteit van het ERM vraagstuk en de omvang van het bedrijf kan het noodzakelijk zijn dat processen worden ondersteund door (min of meer) geavanceerde technieken. Voorbeelden zijn het door middel van procestechnologie "meten van events" in productieomgevingen (storingen, uitval), het geautomatiseerd ondersteunen van het beslissingsproces bij het aangaan van verplichtingen (verstrekken van hypotheken) en het periodiek verzamelen, aggregeren naar doelstellingen en evalueren van testresultaten van beheersingsmaatregelen door de gehele organisatie. Investeringen in dit type technische hulpmiddelen, inclusief de functionele inrichting en technisch beheer en onderhoud, moeten in verhouding staan tot de doelstellingen voor wat betreft actualiteit, transparantie en toegevoegde waarde van het ERM proces.

5 Conclusie en samenvatting

In dit artikel is een overzicht gegeven van een ERM systeem. Een ERM systeem stelt het management in staat om op een transparante wijze om te gaan met risico's die het behalen van de organisatiedoelstellingen bedreigen. Het ERM systeem kent een viertal categorieën van doelstellingen waarbinnen alle organisatiedoelstellingen vallen. Om te komen tot een goed ERM systeem dient het ERM proces te worden doorlopen en zal sprake moeten zijn van een aantal randvoorwaarden. Wanneer een organisatie kan aantonen dat zij over een dergelijk (effectief werkend) systeem beschikt, kan worden gesteld dat deze organisatie in control is. Een in control statement gebaseerd op een ERM systeem geeft aan dat het management haar doelrealisatie serieus neemt en op een verantwoorde wijze tracht de relevante risico's te beheersen. ■

Literatuur

Anthony, R.N. en V. Govindarajan (2002), *Management control systems,* McGraw-Hill/Irwin, New York.

Atkinson, A.A., R.D. Banker, R.S Kaplan en S.M. Young (2001), *Management accounting,* Prentice Hall, New Yersey.

Chapman, C. (2003), Bringing ERM into focus, in: *Internal Auditor*, June 2003, pp. 30-35.

Commissie Corporate Governance (2003), De Nederlandse corporate

governance code: beginselen van deugdelijk ondernemingsbestuur en best practice bepalingen, 9 december, zie: www.commissiecorporate-governance.nl.

Committee of Sponsoring Organizations of the Treadway Commission (1992), Internal Control – Integrated Framework, COSO, Jersey City, zie: www.coso.org.

Committee of Sponsoring Organizations of the Treadway Commission (2004*), Enterprise Risk Management – Integrated Framework,* COSO, Jersey City, zie: www.coso.org.

Emanuels, J., O. van Leeuwen en Ph. Wallage (2004), Internal Control volgens Sarbanes-Oxley: overzicht en praktische betekenis, in: *Maandblad voor Accountancy en Bedrijfseconomie,* jg. 78, no. 7/8, juli/augustus 2004, pp. 348-355.

Emanuels, J. (2005), Interne beheersing: in control of in de krant (beschouwing over een crisis), Oratie Rijksuniversiteit Groningen, Groningen.

Emanuels, J. en W.G. de Munnik (2005), Enterprise risk management als risicobeheersingssysteem, in: *Management Control & Accounting,* jg. 9, no. 6, pp. 30-34.

Paape, L (2003), Enterprise Risk Management Framework, in: *Audit Magazine,* september 2003, pp. 100-102.

Roth, J. en D. Espersen (2002), Categorizing Risk, in: *Internal Auditor*, april 2002, pp. 57-59.

Willemse, R., R. van Rijsewijk en P. Looij, P. (2003), Dynamisch risicomanagement: schieten op een bewegend doel, in: *De Accountant,* jg. 110, no. 3 (november), pp. 44-47.

Noten

1 Dit, en dan nog vrijwel uitsluitend gericht op financiële verslaggeving, is met name het object van Internal Control waar de Sarbanes-Oxley wetgeving zich op richt (Emanuels et al., 2004). Het voldoen aan Sarbanes-Oxley kan uiteraard ook als compliance doelstelling worden gezien.

2 Een ruimere interpretatie van compliance heeft niet alleen betrekking op wet- en regelgeving, maar ook op de normen die de organisatie zelf wenst te handhaven met betrekking tot haar optreden in bijvoorbeeld het economisch en het maatschappelijk verkeer (Emanuels, 2005).